SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2023
ORGANIZATION AND MANAGEMENT SERIES NO. 170

RESEARCH ON STUDENTS' PERCEPTION OF INFORMATION TECHNOLOGY SECURITY – A NEW ERA OF THREATS

Joanna ZARĘBSKA[1*], Natalia HOWIS[2], Małgorzata BARSKA[3]

[1] University of Zielona Góra, Faculty of Economics and Management; j.zarebska@wez.uz.zgora.pl, ORCID: 0000-0002-1655-3086
[2] University of Zielona Góra, student of the Faculty of Social Sciences; howisn@gmail.com
[3] Zielona Góra Police Department: malgorzata.barska@go.policja.gov.pl
* Correspondence author

Purpose: The aim of the article is to diagnose the level of students' awareness about the security of information technology, the risks associated with it, attitudes towards threats and to identify the way of obtaining knowledge about it, protecting oneself against cyber fraud.
Design/methodology/approach: The achievements and results presented in the article were obtained on the basis of literature research and surveys conducted among 119 students. The research technique was a standardized questionnaire completed without the presence of an interviewer via a website.
Findings: On the basis of the obtained quantitative research results, the basic threats related to the use of information technology were identified, the level of students' awareness of cybersecurity and the sources of their knowledge on the subject were assessed.
Research limitations/implications: The analysis of the obtained opinions of students is only a signal of the problem of the needed changes in education on cyber security, threats and opportunities to protect against cybercrime. Research should be extended to other stakeholder groups (e.g. due to age, education, type of work performed) and in a larger area of threats. Competences of students in the field of cybersecurity as future employees are very important, as they affect the willingness to adapt and the level of involvement in new technologies.
Practical implications: The results of the survey have a practical impact on the Police as a source of information on the general knowledge of students in the field of cybersecurity, where they meet it, where they get information about protecting themselves against the threat.
Originality/value: Original research achievements include valuable research results in the area of cybersecurity among the young generation of students. Their knowledge and ability to protect, use and responsibly deal in the area of information technology security is important now and in the future. This ability also indicates gaps and/or appropriate directions of education in the topic in question.

Keywords: information technology security, cybersecurity, online safety, grandson scams.

Category of the paper: research work.

1. Introduction

One of the existential human needs is the need for security. According to Abraham Maslow, this need is on the second level of the hierarchy and refers to the values that concern the security and stability of human life. First of all, it is about job security, stable income, health, peace of mind, resources, moral and family security, and security of private property (Maslow, 2022). The world is developing faster and faster and digitalization is developing along with it. Every aspect of human life is being modernized. According to the Digital Poland Report from 2022, Poland has a very low digitization rate of approx. 40% (while the EU average is 50%). In 2021, out of 27 European Union countries, Poland was ranked 24th in The Digital Economy and Society Index (DESI), which includes 4 pillars in terms of digitization: human capital, connectivity, integration of digital technologies and digital public services, e-government. 'Poles still do not have digital competences, small and medium-sized companies do not use the latest technologies en masse. A number of actions have been taken at national level, but many have not yet been implemented' (Raport Digital Poland, 2022). Despite this, Poles show a positive attitude to change which increases every year. They see them primarily as facilitating everyday life, reducing social inequalities depending on the place of residence and increasing the possibility of finding a better job on the market. The digitization process has definitely changed the service market - it has influenced many decisions of the public and private sectors (Chądrzyński et al., 2021; Saniuk, Grabowska, 2022, pp. 537-547; Załoga, 2022, p. 544).

Digitization significantly facilitates access to medical, financial and educational services. Examples include: the portal "pacjent.gov" or "znanylekarz.pl", thanks to which you can make an appointment with a doctor, have access to the history of our treatment and get an e-prescription in a few steps. Using the "ePuap" portal, you can settle official matters with any administrative authority in Poland that provides such a service from anywhere. All the largest banks currently have their better or worse functioning banking applications for online payments, phone payments, BLIK payments and other financial services (for example, submitting a quick loan application).

Consumer behavior has also been supporting online sales for many years, ranging from grocery shopping to cosmetics, furniture or clothes (Chojnacka, 2021, pp.87-98; Morawski, 2021, pp. 241-257). It is worth noting that often when registering for the newsletter (we are placed in the company's database) we receive a discount on purchases in a given store, new service/purchase proposals, messages about discounts and sales. This is a common practice that encourages purchases on a given platform.

The proper use of digitization of educational facilities such as schools or kindergartens results in better educational results. Implementing new technologies in educational institutions develops individual and group creativity, ensures holistic development and reduces social inequalities (e.g. those related to digital exclusion) (Plebańska, Tarkowski, 2016). In the case

of education, thanks to digitization, a diverse contact of the student with the teachers is possible (via e-mail, direct conversation via Meet in Google Classroom, Zoom, Discord), also student service offices (BOS), the library (ordering books), grants, current events in the life of the university. Both parents (in kindergartens, primary and secondary schools) and students (in universities) have direct access to student attendance or grades (via electronic journal, e-index), admission procedures, etc. It should also not be forgotten that thanks to digitization of education, it was possible to conduct educational classes during the Covid'19 pandemic.

The use of technology and information systems is not only modernity and an advantage of civilization development, but also a threat. The Act of July 5, 2018 on the national cybersecurity system in art. 2, point 4 defines cyber security as "the resistance of information systems to actions that violate the confidentiality, integrity, availability and authenticity of the processed data or related services offered by these systems" (Journal of Laws of 2022, item 1863). In Poland, citizens' data is supervised by the Systems Management Department, whose tasks include, above all, supervision over ICT systems (https://www.gov.pl/web/cyfrizator/departament-zarzadzania-systemami). The Data Management Department (https://www.gov.pl/web/cyfralizacja/departament-zarzadzania-danymi) is responsible for the legal care of the data, the way they are collected and the solutions on how to use them.

Due to the growing level of digitization in Poland, the number of crimes committed remotely using ICT systems has significantly increased (in 2020, 10,420 cybersecurity incidents were recorded, including 73% related to phishing, i.e. extortion of data and/or money by impersonating an invented website, and in 2021 22,575 events were recorded - 76% concerned phishing) (Report ... CERT 2020, p. 13; Report ... CERT 2021, p. 12).

Until recently, one of the most popular fraud methods was the so-called. "keylogger" (Trejderowski, 2013), which in 2022 could even be considered "obsolete". Keylogger comes in many forms. This is a type of program or device that registers keystrokes. Today, every Internet user can effortlessly buy an online keylogger in the form of a flash drive, which records activities as long as it is connected to the device. This program can show in real time what someone is typing on the keyboard, including mainly passwords for access to, for example, a bank or e-mail. As malicious programs are also developing rapidly, today the hacker/scammer does not have to sit in front of the computer, the program can save all keyboard actions in a separate file. However, it usually required physically inserting the flash drive into the device, which forced the fraudster to construct a strategy on how to do it.

The public's awareness of the immediate reaction in the event of loss of documents (identity card, passport and other sensitive information, such as PESEL) is certainly a success (Kondek, Ożarowska, 2022a). The report of the Polish Bank Association and the Police Headquarters shows that the number of attempts to use someone else's document or forge documents is definitely decreasing every year. Thanks to this, in the last year of 2021, illegal taking of 7,885 loans for a total amount of PLN 245.2 million was prevented in Poland (Kondek, Ożarowska, 2022b). Unfortunately, the data of the National Police Headquarters show that in 2021 there

was no province in Poland where there would be no fraud using the "grandson" and "policeman" methods. At least 1,176 elderly people lost their life savings in the first half of 2021, and the losses amounted to over PLN 63 million (http://bip.kgp.policja.gov.pl/).

One of the forms of fraud is impersonating employees of public trust. Gentlemen dressed as policemen or employees of a housing cooperative could appear directly in front of the door to our apartment. This type of fraud, as a result of digitization, turned into phishing, consisting in extorting data and/or money by impersonating a made-up website (Trejderowski, 2013). Much more often, scammers use a negative message, they want to evoke a sense of fear in the recipient, which will make it more likely that he will not think twice before clicking on the link. This feeling is evoked by sending the recipient information about a fraud attempt, failure to pay for the purchase, or failure to receive the transfer. The user clicks on a link that redirects him to a page identical to the original page, enters his details (e.g. bank details) and thus makes a transfer to the scammer. The same method is used by phone, i.e. we get a "phone call from the bank" that a suspicious transfer has been detected or our account has been blocked, so the "bank employee" asks us to enter the password or PIN to the card to confirm our identity. Such a situation will never actually happen - the bank will never ask us for passwords over the phone. When we are not sure who is on the other end of the call, it is safest to hang up and contact the bank to clarify the situation.

Today, the police are flooded with fraud reports "via BLIK" or SMS "Pay for a package". The Department of Cybersecurity in Poland creates and implements a strategy for protection in cyberspace, and directly supervises the National Cybersecurity System, which since 2018 ensures the protection of digital services and supervises the achievement of a high level of security of ICT systems. At the end of 2021, due to the growing number of crimes related to cyberspace, the Central Office for Combating Cybercrime was established. Its primary tasks include detecting, combating and preventing crimes in the ICT network (https://cbzc.policja.gov.pl/).

Every day, more and more data is placed on the Internet (Chądrzyński et al., 2021). This process is called dataification. These are data of various origins, for example: from IT systems, individual, business and institutional users, from databases of private companies and institutions. It is worth mentioning when explaining this process that nothing is free on the Internet. By providing the phone number, our email, we "pay" with our data, which are placed and used in various databases. It is worth remembering that we place a significant amount of information ourselves. Thanks to portals such as Facebook, Linkedin, Instagram, we can find out, for example, how the user's education was conducted, where he currently works, what is his phone number or email address and where is he currently located? The thief no longer has to wait for an opportunity in front of the house, watch the apartment for weeks to know the schedule of the day, just visit Internet profiles. It is worth mentioning that we often bring the threat to ourselves completely unintentionally (Balibok, Matras, 2014). Such behaviors include delegating access authorizations (e.g. sharing bank login details with

another person), setting a weak password and not changing it, ignoring security rules, e.g. access control in buildings. Creating strong, complicated passwords annoys users. The need to remember passwords with many requirements - uppercase, lowercase, special characters. The biggest mistake is creating a password that we use for many login pages and creating an easy password using information that is easy to find about us (such as names of children, animals or date of birth) (Sajler-Fudro, 2022). With this information, it is enough to use a password cracker (e.g. John The Ripper), which any user can download for free using a web browser. How to create a password then? The longer the password, the longer it will take for fraudsters to guess it. Special characters make it harder for programs to guess your password. However, the best password is a meaningless password, such as Jk4lW.35jh?

Today's mobile phones include payment options, i.e. we can pay using applications thanks to near field communication (NFC) technology or pay thanks to the built-in radio frequency identification (RFID) portable payment card. An interesting, one of the modern types of fraud is neurohacking (Kotz et al., 2015). It involves remote hacking of devices necessary for the patient's life, such as an insulin pump or a pacemaker. These devices collect sensitive data about the patient and can easily become the subject of a crime (e.g. forcing the patient's ATM card data with the threat of turning off the device or administering a high dose of insulin that threatens life). At the same time, it can be useful if you want to mislead the Police institution or destroy evidence in the form of switching off, blocking access to the device or changing the data stored in it.

The article presents the results of a survey on the assessment of young people's awareness of the security of information technology, the risks associated with it and the way of obtaining knowledge about it. 119 students took part in the study, mostly young people aged between 18 and 27 (so-called Generation Z or Generation C) (Rojewska, 2019). This generation is considered the first people growing up in a fully digitized society, therefore it is assumed that they are people with a certain level of familiarity with modern computer equipment, smartphones, tablets, etc. These people have no problems with fear of new information technologies and feel good in their surroundings (they can't even imagine life without them).

2. Materials and metods

The conducted research consisted of two parts. The first part of the research consisted of literature analysis. A systematic review of the literature on the subject and a critical analysis of the content of selected publications made it possible to identify the problem and the research gap. Additional support in identifying the problem and formulating questions was the professional experience of the research co-author (as an expert).

In the second part of the study, survey questions were formulated and an online survey (CAWI - Computer-Assisted Web Interview) was conducted among students (https://forms.gle/RSYncU2DYWQvsaaY9). The basis of the pilot study was a questionnaire containing 11 open and closed questions with the possibility of giving one or more answers.

The survey was conducted among 119 students in the last few months of 2022 (from November 1, 2022 to December 31, 2022). Purposeful selection of the group was used. The respondents were university students (full-time and part-time) from various cities and fields of study. The study included 77 women (64.7%), 40 men (33.6%) and 2 people (1.7%) who did not declare their gender to the above groups. Since the study was conducted over a short period of time and most of the respondents are students of the University of Zielona Góra (almost 70%), it should be treated as a pilot study and not related to the entire population of young Poles, but to representatives of a certain group of them.

3. Research results

The survey conducted in 2022 was filled in mainly by students from Lubuskie - 83 people (69.7%), Dolnośląskie 14 people (11.8%), Mazowieckie and Wielkopolskie voivodships - 5 people each, Pomorskie, Śląskie and Zachodniopomorskie - 3 people each, Łódzkie, Małopolskie and Świętokrzyskie - 1 person each (in total from 10 out of 16 voivodeships). Among 119 students, only 11 are in technical faculties (e.g. Faculty of Mechanical Engineering, Faculty of Computer Science, Electrical Engineering and Automatics) and the remaining 108 are in humanities (e.g. Faculty of Economics and Management, Faculty of Social Sciences, Faculty of Psychology, Faculty of Pedagogy, Faculty of Nursing, Faculty of Veterinary Medicine). Most of the respondents live in rural areas - 28.6%, in cities of up to 50,000 inhabitants. inhabitants live in 26.1%, the third place is 24.4% of respondents living in medium-sized cities (100-500 thousand inhabitants), 11.4% are inhabitants of large cities (over 500 thousand inhabitants), and 9.2% are inhabitants of cities with a population between 50-100 thousand More than half of the respondents are first and second year students, i.e. those under 21 (52.1%), between 22 and 25 there were 36.1% of the respondents, and the rest are people over 26 (11.8%).

Most students, 57.1%, have dealt with fraud as victims (25.2%) or people who wanted to cheat (31.9%), but thanks to reflexes and resourcefulness they avoided fraud - compare figure 1. Other students (42.9%) do not remember or have not been victims of fraud. Nevertheless, out of the group of 119 students surveyed, 76.5% of them answered that they knew people who were victims of fraud (usually a family member or friend).

Figure 1. Students exposed to fraud.

Source: own study.

In addition, as shown in Figure 2, most students heard about scams using the "grandson" (90.8% - 108 people), "cop" (83.2% - 99 people), they also received "unknown links, e.g. in an e-mail" (90.8% - 108 people), "unknown links sent to the phone" (86.6% - 103 people), related to lotteries or prizes (79.8% - 95 peole), impersonating a "bank employee" (68.9%), by installing a virus (68.1%), related to prepayments, e.g. on OLX (61.3%), using the BLIK method (60.5%), impersonating a "ZUS employee" (31.1%), impersonating a "housing cooperative employee" (22.7%), and single cases of an attempt to extort data/money by a person impersonating a person associated with charity or cryptocurrency activities.

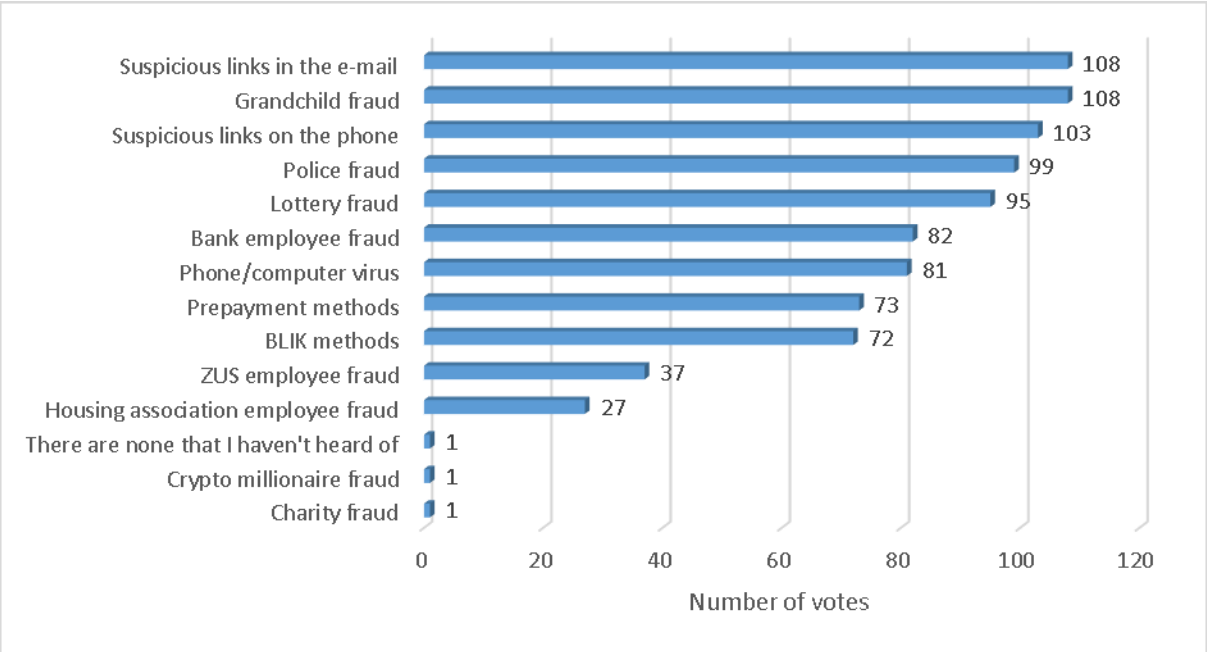

Figure 2. Fraud or extortion of money, confidential information that the respondents heard about.

Source: own study.

Where students obtain information on counteracting fraud can be found in the answers listed in Figure 3. They most often obtain information on this subject from the Internet (85.7% - 102 people), from friends and family (68.1% - 81 people), from television (44.5% - 53 people) and from bank website (40.3%), school/university website (34.5%), radio website (28.6%), official websites, e.g. Police (27.7%), press (16.8%).

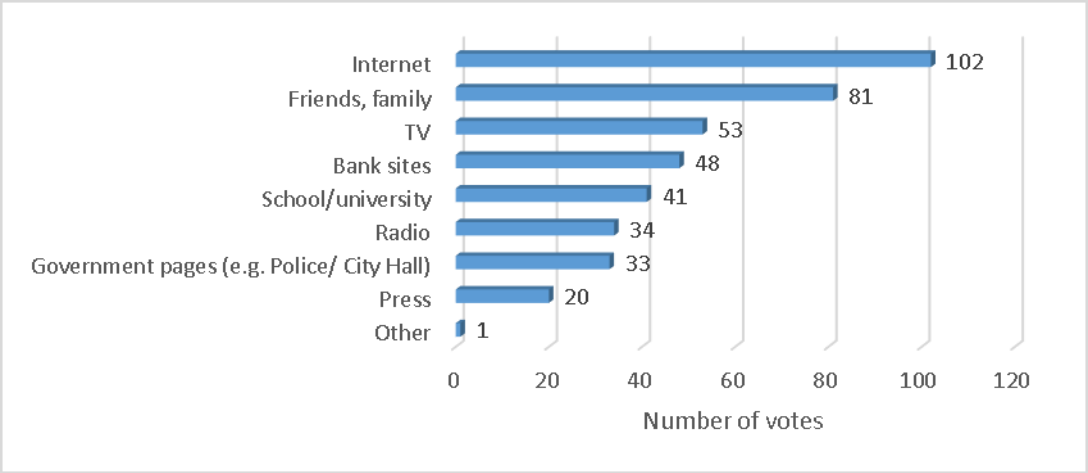

Figure 3. Collecting anti-fraud information.

Source: own study.

Students were asked to tick the answers related to the devices they trust the most when making various financial transactions. As it turns out (figure 4), students have the greatest trust in payments via a computer/laptop (30 people - very high and 40 - high sense of security), followed by Blik payments (32 people - very high and 33 - high sense of security), payments via phone (26 - very high and 34 - high sense of security), and the least trust in payments via tablet (7 and 20 respectively) and watch (8 and 12 respectively).

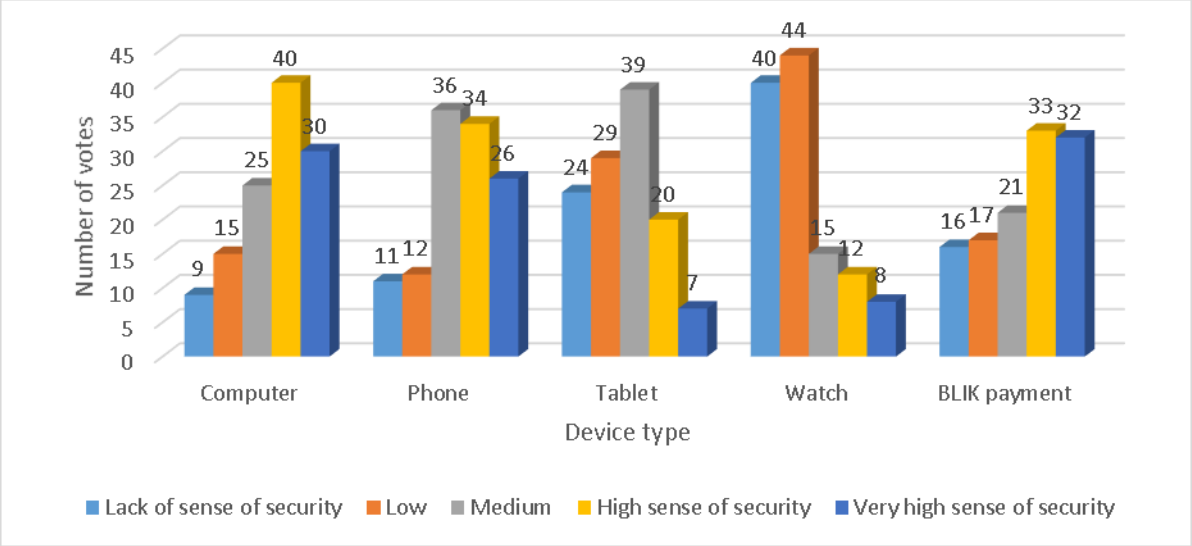

Figure 4. Devices students trust the most when making financial transactions.

Source: own study.

The computer/laptop inspires the greatest trust and sense of security among students, but it is also due to the fact that 81.5% (97 people) have an anti-virus program installed on these devices (figure 5). Only 48.7% (58 people) of students have an antivirus installed on their phone. The lack of adequate protection against viruses is certainly the reason for the lack of trust in making payments with other devices, which was shown earlier in figure 4.

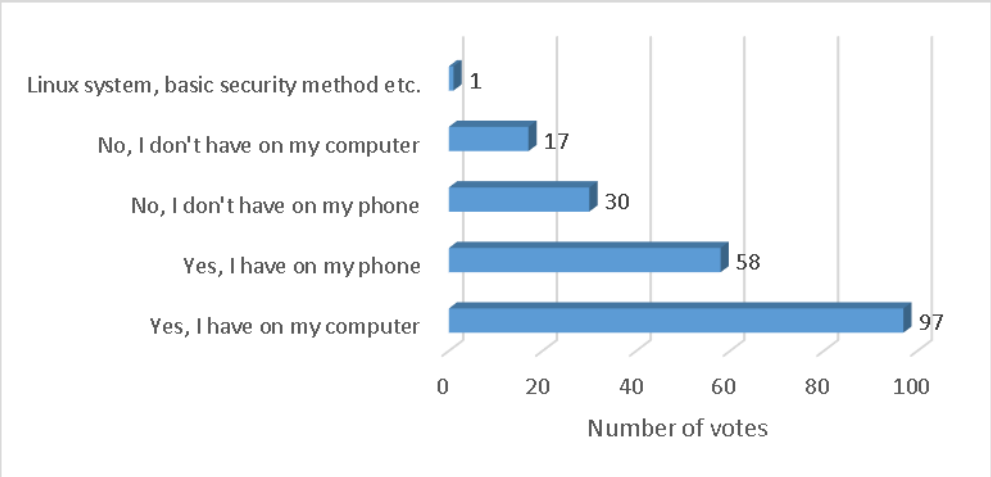

Figure 5. Devices on which students have an antivirus program installed.

Source: own study.

A n important element that banking websites or applications remind us of is the frequent change of passwords with an appropriate number of complex characters. It is also an important factor of a sense of security in the use of modern information technologies. As it turns out, 31.1% of students change their password as soon as they are reminded of it by the website/store where they are logged in (figure 6). It is alarming that 19.3% of students do not change their passwords at all, and 15.1% do it once every few years (they make up a total of 34.4% of the respondents), 14.3% of the respondents change their passwords on average once a quarter, 11.8% - once a year, and only 6.3% - once a month and 2.1% - once a week.

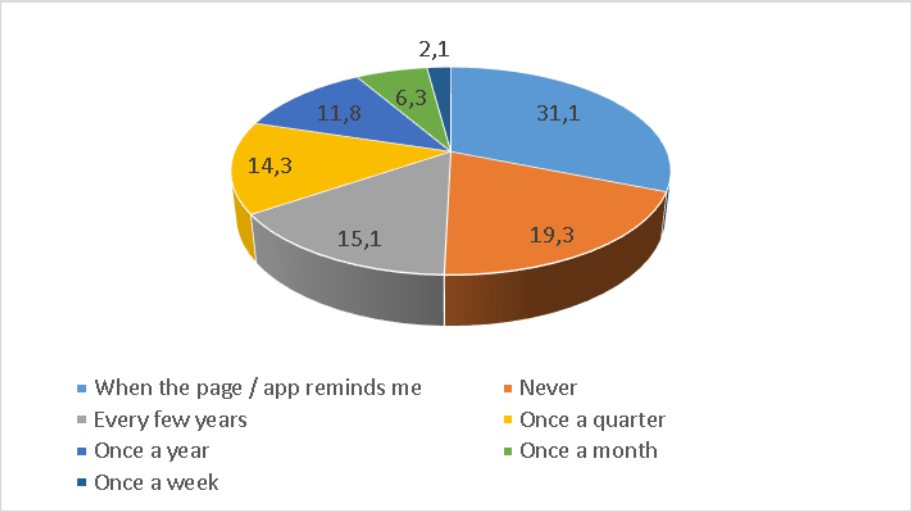

Figure 6. Password change frequency [%].

Source: own study.

Many students, as many as 31.1%, very often use the same password for many accounts, often - 28.6%, and some even always - 3% (total 62.7%). The second group are students who rarely use the same password for many accounts and they constitute a group of 20.2% of the respondents, very rarely - 8.7%, never - 8.4% (37.3% in total) - figure 7.

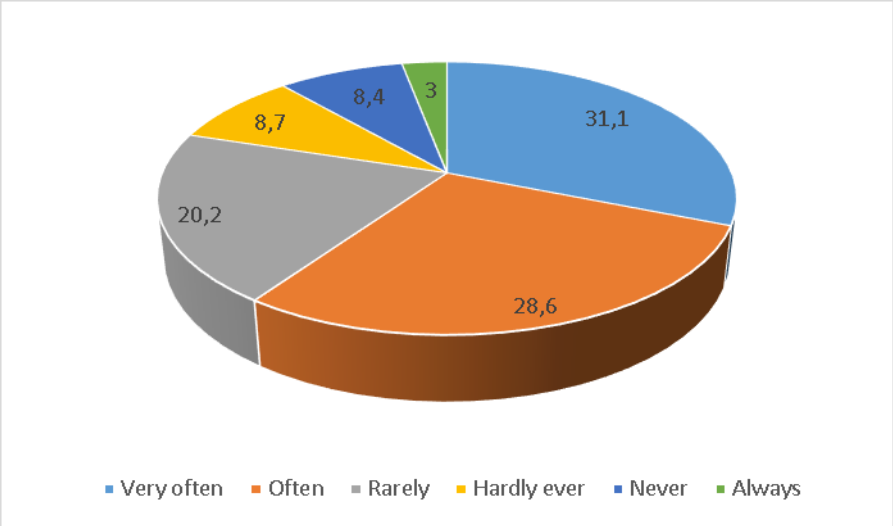

Figure 7. Frequency of using the same password for multiple accounts [%].
Source: own study.

The high frequency of using the same password for many accounts results from the problem of remembering a large number of passwords and a large number of accounts (computer, social networks, online stores). Figure 8 summarizes students' responses to writing down passwords in notebooks, calendars, or cards. It turns out that 43.7% of students do not save their passwords, and 10.1% used to write them down and now do not (they make up a group of 53.8% of the respondents). The remaining 46.2% of respondents save passwords to varying degrees so as not to lose them.

The next question concerned students who save their passwords in a computer/laptop browser so that there is no need to remember them or write them down on paper/calendar. This activity is always performed by 7.6% of students. 35.3% of students save their passwords in the browser frequently, 34.5% do it sometimes and 22.6% never do it.

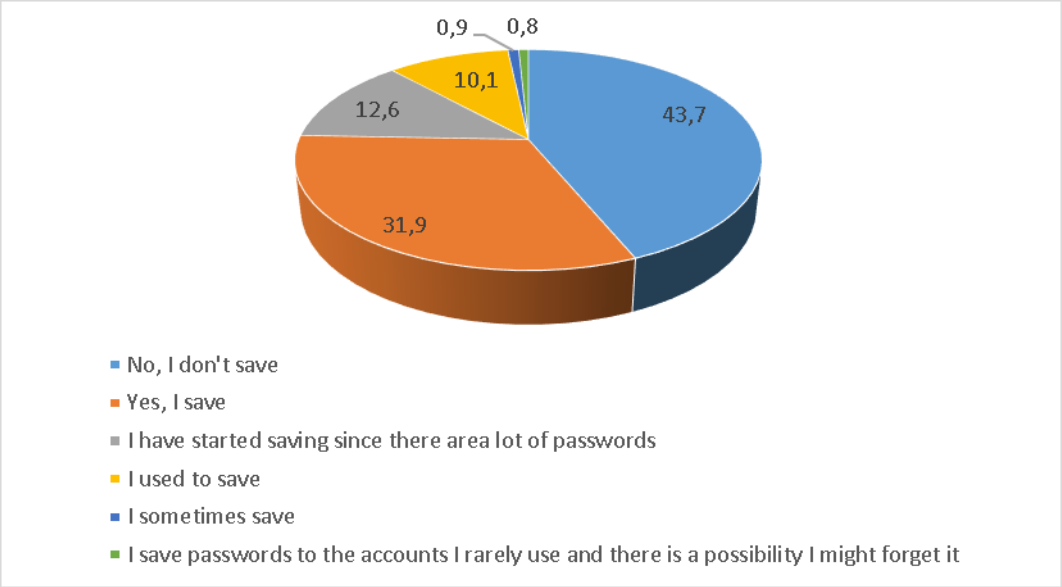

Figure 8. Saving passwords in notebooks, calendars or on cards [%].

Source: own study.

The problem in the case of saving passwords in the browser of a computer/laptop may be damage to the website or a change of computer, because then the password will not be remembered. For young people, however, this is not a big problem, because in this case, for example, they recover lost passwords or create a new account with a new password.

4. Summary

The research described in this article are declarations of young people who are currently students of universities in Poland, who are between the ages of 18 and 27 (so-called Generation Z or Generation C). This generation grew up in a fully digitized society, therefore operating a computer, smartphone, tablet or watch (smartband) is not a problem for them and does not arouse fear (as in the case of older people).

The surveyed students have knowledge about various types of fraud and more than half (57.1%) have encountered them in person or at someone's family/friends (76.5%). They have the greatest confidence in computers/laptops (70%), which most often have pre-installed virus protection programs, and the least in watches (20%). Young people, despite being aware of the threats, do not care about cybersecurity, have no problem with technological innovations and actually consciously expose themselves to fraud (18.5% do not have an anti-virus program on a computer believed to be the safest device for financial transactions). Even if students do not change their passwords very often, they write them down on cards or on a computer in a browser. It is not very secure, but each user chooses the most convenient form of recording for himself.

Since 25.2% of students have dealt with fraud as victims, the need for further education of the young generation in the field of cybersecurity and modern information technologies as a new threat is clearly visible. Most of the surveyed students will soon become graduates of first or second degree studies and start working. The future employer will probably be interested in an employee who can operate modern IT devices, but also cares about their security and shared data.

References

1. Balibok, P., Matras, A. (2014). Bankowość mobilna jako innowacyjny kanał dostępu do usług bankowych. *Rocznik Ekonomii i Zarządzania, tom 6(42), nr 2,* pp. 7-22.
2. Centralne Biuro Zwalczania Cyberprzestępczości. Retrieved from: https://cbzc.policja.gov.pl/, 2.01.2023.
3. Chądrzyński, M., Gruziel, K., Kacperska, E., Klusek, T., Utzig, M. (2021). *Polska w dobie cyfryzacji*. Warszawa: SGGW.
4. Chojnacka, M. (2021). *Organizacja przyszłości*. Gorzów Wielkopolski: Wydawnictwo Akademii im. Jakuba z Paradyża.
5. Departament Zarządzania Danymi. Retrieved from: https://www.gov.pl/web/cyfryzacja/departament-zarzadzania-danymi, 21.12.2022.
6. Departament Zarządzania Systemami. Retrieved from: https://www.gov.pl/web/cyfryzacja/departament-zarzadzania-systemami, 21.12.2022.
7. Komenda Główna Policji. Retrieved from http://bip.kgp.policja.gov.pl/, 2.11.2022.
8. Kondek, G., Ożarowska, E. (2022a). *Raport o dokumentach infoDOK (2 kwartał 2022*). 50 edycja. Retrieved from: https://zbp.pl/Aktualnosci/Wydarzenia/Raport-InfoDOK,-II-kw-%E2%80%93-maleje-liczba-prob-wyludzen-kredytow, 20.12.2022.
9. Kondek, G., Ożarowska, E. (2022b). *Raport o dokumentach infoDOK (3 kwartał 2022*). 51 edycja. Retrieved from: https://zbp.pl›infodok-2022-07-09-wydanie-51(1).pdf, 20.12.2022.
10. Kotz, D., Fu, K., Gunter, C., Rubin, A. (2015). Security for mobile and cloud frontiers in healthcare. *Communications of the ACM. Vol. 58, Iss. 8*, pp. 21-23.
11. Maslow, A.H. (2022). *Motywacja i osobowość*. Warszawa: PWN.
12. Morawski, J. (2021). Logistyka ostatniej mili - usprawnienia w obsłudze klienta. *Przedsiębiorczość i Zarządzanie*, *tom 22, zeszyt 2,* pp. 241-257.
13. Plebański, M., Tarkowski, A. (2016). *Cyfryzacja polskiej edukacji. Wizja i postulaty*. Retrieved from: https://centrumcyfrowe.pl/wp-content/uploads/2016/07/cyfryzacja-polskiej-edukacji_final.pdf, 20.12.2022.

14. Raport Digital Poland (2022). *Technologia w służbie bezpieczeństwa. Czy Polacy zostaną społeczeństwem 5.0? Edycja 2022,* Retrieved from: https://digitalpoland.org/publikacje/pobierz?id=602693cf-262c-4f2a-bfa3-9f91cfaffd3c, 2.01.2023.
15. Raport roczny CERT Polska 2020 (2021). *Krajobraz bezpieczeństwa polskiego internetu*. Warszawa: NASK PIB/CERT Polska.
16. Raport roczny CERT Polska 2021 (2022). *Krajobraz bezpieczeństwa polskiego internetu*. Warszawa: NASK PIB/CERT Polska.
17. Rojewska, M. (2019). *Milenialsi, pokolenie Z, Y, X, generacja baby boomers – kto to?* Retrieved from: https://interviewme.pl/blog/pokolenie-z, 5.10.2022.
18. Sajler-Rudro, P. (2022). Zagrożenia bezpieczeństwa w użytkowaniu systemów informatycznych – klasyfikacja i metody zapobiegania. *Nauki Ekonomiczne, tom 35,* pp. 189-214, DOI: 10.19251/ne/2022.35(11).
19. Saniuk, S., Grabowska, S. (2022). Development of Knowledge and Skills of Engineers and Managers in the Era of Industry 5.0 in the Light of Expert Research. *Scientific Papers of the Silesian University of Technology. Organization and Management Series, no. 158*, pp. 537-547. DOI: 10.29119/1641-3466.2022.158.35
20. Trejderowski, T. (2013). *Kradzież tożsamości. Terroryzm informatyczny*. Warszawa: Eneteia.
21. Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych [Dz.U. 2022, poz. 1863].
22. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne [Dz.U. 2021, poz. 2070].
23. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa [Dz.U. 2022, poz. 1863]**.**
24. Załoga, W. (2022). Digital competences of the information society era in the aspect of safety in cyberspace. *Scientific Papers of Silesian University of Technology. Organization and Management, No. 164,* pp. 541-552. DOI: http://dx.doi.org/10.29119/1641-3466.2022.164.41.